II. AMENDMENTS TO THE SPECIFICATION:

Please make the following amendments to the specification:

On page 10, line 9 through page 11, line 2, please amend as follows:

In previous systems, the solution was to manually write filters that permit IKE traffic to pass. Such a task, however, is often a laborious and error-prone task, particularly for a number of VPN connections such as nested connections and nested ~~confections~~ connections with coincident local endpoints. The present invention obviates the need for such filters. Specifically, under the present invention, filter detection system 26 first searches VPN gateway node 10 for IKE traffic permit filters. If no such filters are detected, IKE traffic enablement system 28 will allow VPN gateway node 10 to send and receive IKE traffic freely (subject to any limiting inbound filters in place). In a typical embodiment, filter detection system 26 will be run every time rules are loaded or uploaded to VPN gateway node 10. If IKE traffic permit filters are not detected, IKE traffic enablement system 28 will automatically allow IKE traffic to pass. Conversely, if IKE traffic permit filters are detected, IKE traffic will be handled according to the rules and filters of VPN gateway node 10. This allows system administrators of the VPN to choose whether to handle IKE traffic explicitly with manually written filters, or to allow the system to automatically handle IKE traffic.